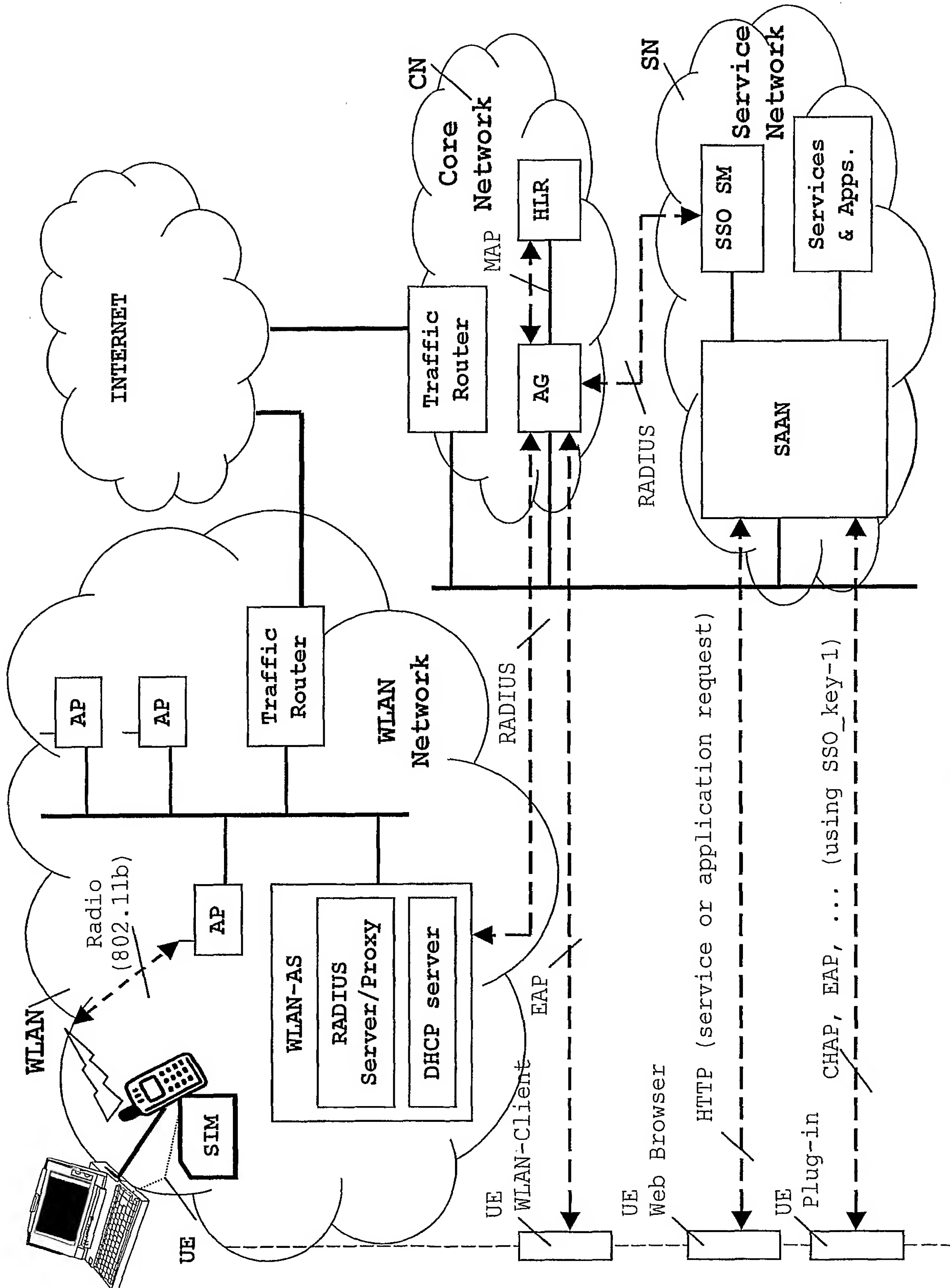stored at the user's equipment, includes a step of downloading an SSN plug-in from an entity (SAAN, SSO_SM) in the service network (SN), the SSO plug-in running for confirming back the user's shared key (SSO_key-2).

26. The method of claim 21, wherein the step of confirming (S-32, S-33) the second user's shared key (SSO_key-2) stored at the user's equipment, includes a step of processing the user's shared key (SSO_key-2) to obtain a key code (MAC(SSO_key-2)) to be transmitted to an entity (SAAN, SSO_SM) in the service network (SN).

27. The method of claim 26, wherein the step of verifying (S-34) whether the second user's shared key (SSO_key-2) matches the first user's shared key (SSO_key-1) includes a step of processing at an entity (SAAN, SSO_SM) of the service network (SN) the first user's shared key (SSO_key-1) to obtain a first key code (MAC(SSO_key-1)) to be matched against a second key code (MAC(SSO_key-2)) originated from the user's equipment.

28. The method of claim 21, wherein the step of creating (S-301) a master session for the user at the entity (SAAN, SSO_SM) in the service network includes a step of receiving the first user's key (SSO_key-1) from an entity (AG) of the core network (CN).

29. The method of claim 21, wherein the step of creating (S-301) a master session for the user at the entity (SAAN, SSO_SM) in the service network includes a step of initiating an access session (S-29) when the user accesses the access network.
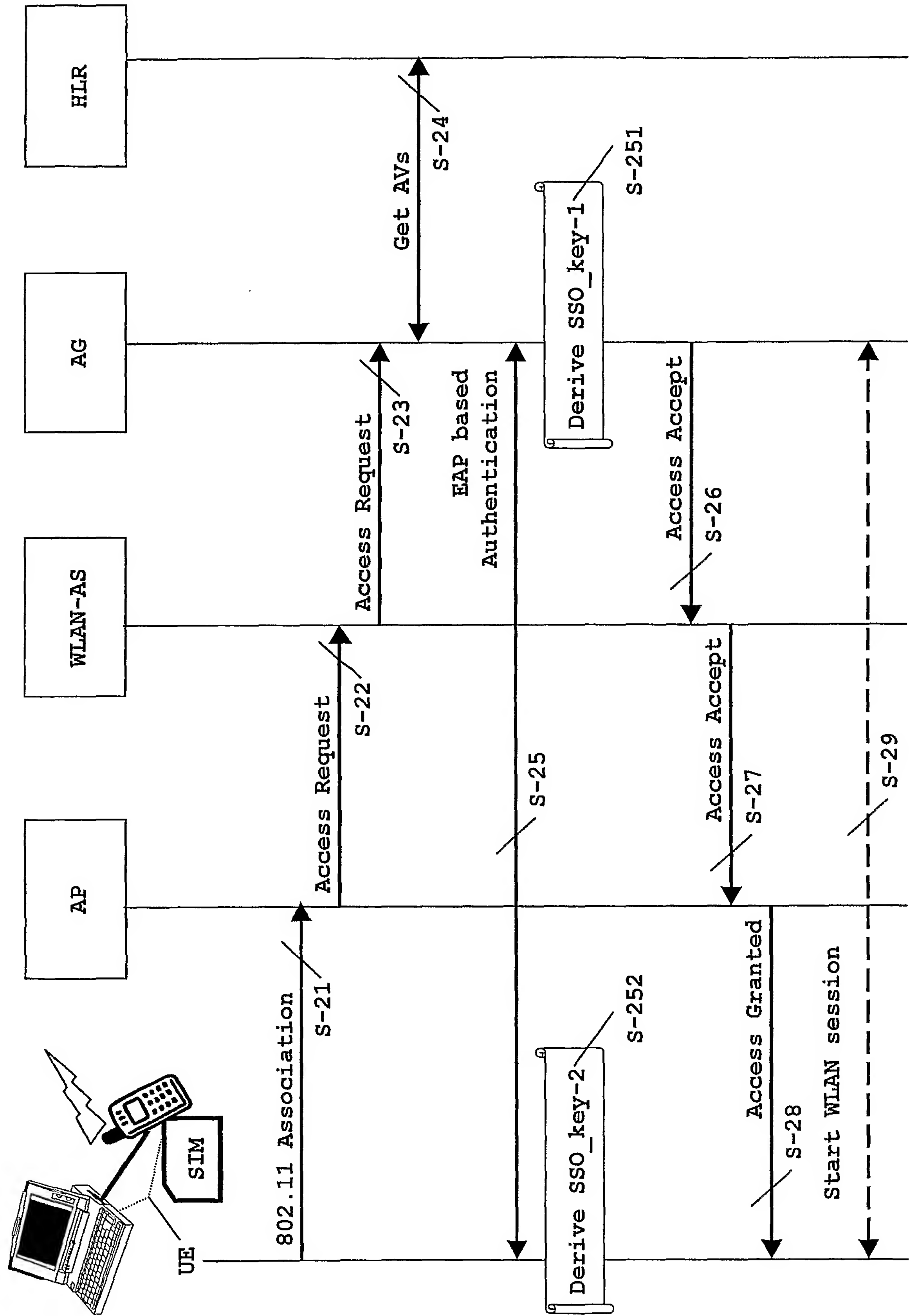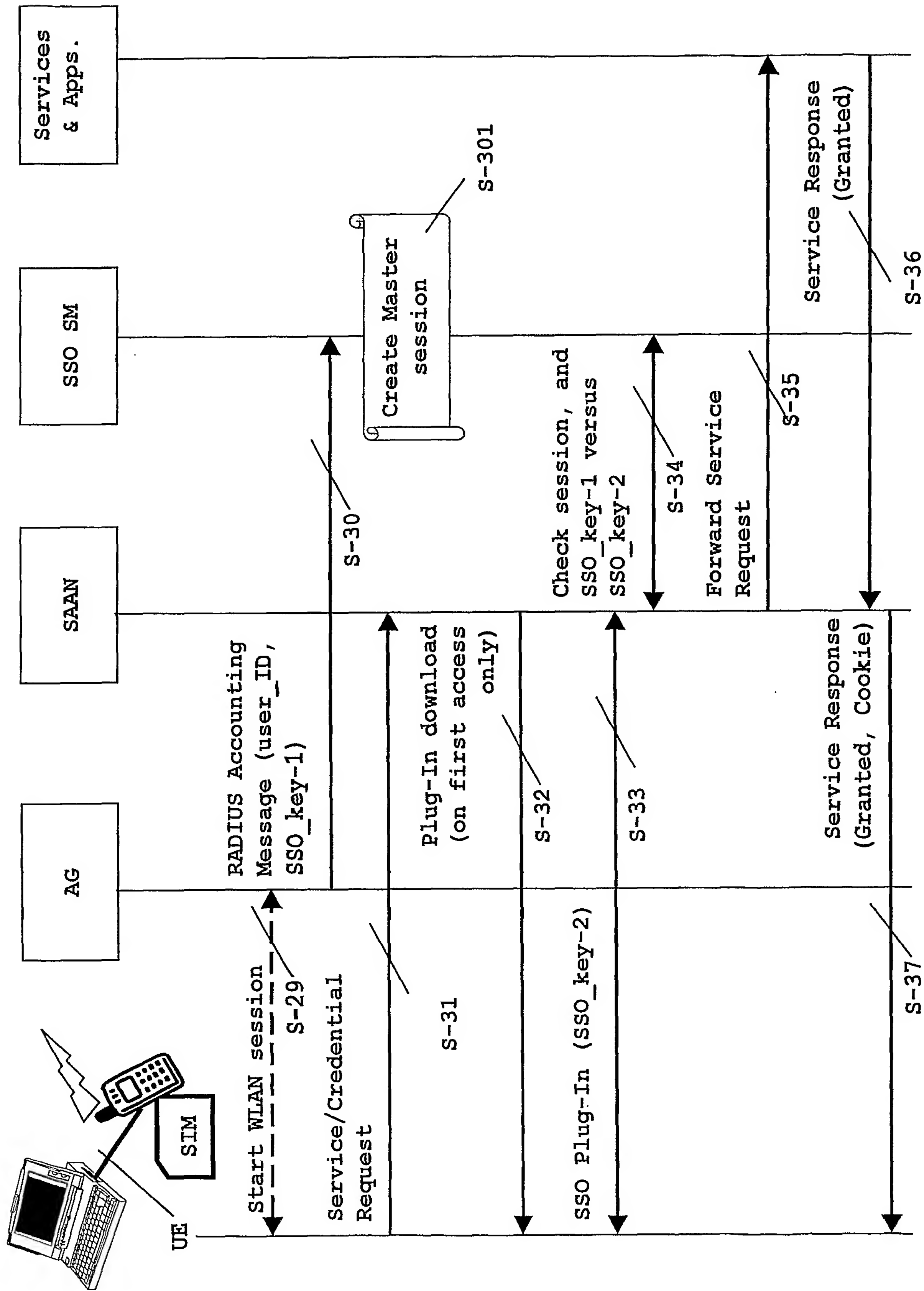
FIG.-1-

FIG.-2A-

FIG. -2B-